U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE

HEARING CHARTER

Cybersecurity Education – Meeting the Needs of Technology Workers and Employers

Wednesday, July 21, 2004
10:00 a.m. - Noon
2318 Rayburn House Office Building

1. Purpose

On Wednesday, July 21, 2004, the House Committee on Science will conduct a hearing to review efforts by academia, industry and government to develop a cybersecurity workforce.

2. Witnesses

Mr. Chet Hosmer is the President & CEO of WetStone Technologies, Inc. of Cortland, New York. Mr. Hosmer has taught Network Security and Cyber-Crime and Computer Forensic courses at Utica College, and he is the Research Advisor for the Computer Forensics Research and Development Center of Utica College. Mr. Hosmer also is co-chair of the Electronic Crime and Terrorism Partnership Initiative's Technology Working Group at the National Institute of Justice.

Mr. John Baker is the Director of Technology Programs for the Division of Undergraduate Education of the School of Professional Studies in Business and Education at the Johns Hopkins University in Baltimore, Maryland.

Mr. Erich Spengler is the head of the Regional Center for the Advancement of Systems Security and Information Assurance at Moraine Valley Community College in Palos Hills, Illinois.

Second Lieutenant David Aparicio is an electrical engineer for the Air Force Research Laboratory Information Directorate in Rome, New York. Lt. Aparacio is a graduate of the "Cybersecurity Boot Camp" run jointly by the Air Force, Syracuse University, the New York State Office of Science, Technology and Academic Research.

Ms. Sydney Rogers is the head of the Regional Center for Information Technology at Nashville State Community College in Nashville, Tennessee. Ms. Rogers is also the Vice President for Community and Economic Development at the community college and her responsibilities include workforce development, computer services and distance education.

3. Overarching Questions

The hearing will address the following overarching questions:

- How are academia, industry and government working together to meet the Nation's cybersecurity education and training needs?

- What are the strengths and weaknesses of existing cybersecurity education and training programs?

- What new and emerging challenges need to be addressed in this area? How can the federal government contribute to this effort?

4. Brief Overview

- Information technology systems play a critical role in today's economy, yet they are vulnerable to security breaches and attacks. Adequately protecting these systems requires, among other things, a well trained cybersecurity workforce to block, detect and counter any threats to vital computer systems and networks.

- In 2002, the President signed into law the *Cybersecurity Research and Development Act* (P.L 107-305), which originated in the Science Committee. The Act effectively designated the National Science Foundation (NSF) as the lead agency for civilian cybersecurity research and education, and it authorized $216 million over FY2003 - FY2007 for NSF cybersecurity education and training programs. The Act also authorized advanced cybersecurity education and training programs at the National Institute of Standards and Technology (NIST), but these programs have never been funded.

- The National Security Agency (NSA) also is engaged in cybersecurity education and training. In addition, the Department of Homeland Security (DHS) supports public awareness and outreach on cybersecurity vulnerabilities and countermeasures, and it helps coordinate private-sector efforts with those of the federal government.

- As the challenges of cybersecurity emerge and evolve, so too do the courses and programs of cybersecurity education and training. From programs in traditional settings, like two- and four-year colleges and universities, to other programs, like the Cybersecurity Boot Camp, the cybersecurity education and training continuum is growing and becoming more standardized in its effort to meet the needs of technology workers and employers.

4. Background

Estimates of annual economic losses caused by computer virus and worm attacks and to hostile digital acts in general run from about $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks). While the precise figures are open to question, there is no doubt that cybersecurity intrusions result in significant losses due to downtime, lost productivity, and expenses related to testing, cleaning and deploying patches to computer systems.

Experts increasingly point out that improving cybersecurity requires cybersecurity training for technicians and users, in addition to promulgating sound security practices and deploying sophisticated technology. As one security professional explained, you can be "bristling with firewalls and IDS (intrusion detection systems), but if a naïve user ushers an attacker in through the back door, you have wasted your money."

Education and Training Needs

Many system failures and security breaches occur because of human error. Employees may fail to install a patch, or configure a firewall incorrectly, or otherwise leave a system open to intrusion. Such errors occur, in part, because responsibility for security traditionally has fallen to non-security workers who may lack the time, training and focus to handle such responsibilities.

A 2002 report by the National Workforce Center for Emerging Technologies and the Computing Technology Industry Association (CompTIA) found that many security organizations were beginning to seek security professionals, deciding that it was no longer acceptable just to buy a firewall package, install it, and let it run.

Industry is also increasingly interested in fostering concern with cybersecurity at all the levels of the workforce dealing with computers from administrative workers (such as network administrators, technicians, and help desk staff) to engineers (including software developers) to system architects.

Responding to that interest, cybersecurity education and training is increasingly being offered through degree-granting programs at both two- and four-year colleges and universities, but also through shorter, credit and non-credit programs that provide certificates or provide background for students to pass certification exams.

Federal Support for Cybersecurity Education and Training

National Science Foundation

Federal Cyber Service: Scholarship for Service (SFS)—The program has two aspects – a "Scholarship Track" that provides grants to colleges and universities for student stipends, and a "Capacity-Building Track" that provides grants to colleges and universities to improve their ability to provide courses in cybersecurity.

The Scholarship Track provides four-year grants to colleges and universities, which, in turn, use the money to provide as many as 30 two-year scholarships. In exchange for two years of stipends ($8,000 per year for undergraduate students and $12,000 for graduate students) and a summer internship at a federal agency, participating students are required to work for two years in the Federal Cyber Service for a federal agency. Since 2001, 391 individuals have participated in the scholarship program.

The Capacity Building Track provides two-year grants of up to $150,000 per year for such activities as adapting and implementing the use of educational materials, courses or curricula; offering technical experience; developing laboratories, and offering faculty development programs. (An additional $150,000 per year is available to partnerships that include minority serving institutions).

The SFS program was funded at $16.1 million in Fiscal Year (FY) 2004, and the Administration request for FY 2005 is $16.2 million. A list of colleges and universities participating in the SFS program is provided in Appendix II.

Advanced Technology Education (ATE)—ATE is NSF's program to improve technical education at two-year colleges. Grant awards may involve partnerships between two-year and four-year institutions.

One aspect of ATE is the funding of regional centers (such as the two giving testimony at this hearing), which are designed to create model programs in specific areas, such as cybersecurity, to adapt those programs to local needs, provide professional development for college faculty, and help recruit, retain and place students.

The ATE program, which received $45.23 million in FY2004, of which about $3.7 million will be invested in cybersecurity education and training (although the breakdown for cybersecurity is a very rough estimate).

National Security Agency

The National Security Agency (NSA) established the Centers of Academic Excellence in Information Assurance Education (CAE/IAE) Program in 1998 to increase the number of professionals with information assurance expertise in various disciplines. The CAE/IAE Program endorses qualified four-year and graduate information assurance degree programs (including those at Johns Hopkins, which is testifying at this hearing).[1] Currently, there are 59 universities in 27 states that are designated as CAE/IAE (see list in Appendix III). Being designated a CAE/IAE does not guarantee an institution funding,

[1] Prospective institutions must meet rigorous standards to receive the national recognition and the CAE/IAE designation, including courseware that is certified under the National Security Telecommunications and Information Systems Security Standards as well as ten other criteria describing dimensions, depth and maturity of the information assurance program.

but it is a "seal of approval" that facilitates applying to grant programs, and it makes institutions eligible for certain NSA programs.[2]

NSA also manages an SFS program in information assurance for the Department of Defense (DOD). This program is similar to the one run by NSF, with scholarships provided for study at a CAE/IAE in return for a student's service at a DOD agency. Currently 82 students are participating in the NSA SFS program.

Department of Homeland Security

The Department of Homeland Security (DHS) is working to increase cybersecurity awareness, foster cybersecurity training and education programs, and promote private sector support for well-coordinated, widely recognized professional cybersecurity certifications. In these areas, DHS plays a supporting role, consulting on the efforts and programs underway in other government agencies, at universities, and in the private sector.

5. Witness Questions

Questions for Mr. Hosmer

- In your experience, what knowledge and skills are currently needed in the cybersecurity workforce? Have cybersecurity education and training programs been sufficiently flexible to respond to these needs as well as the needs of traditional and returning students?
- What are the current strengths and weaknesses in cybersecurity education and training programs? Do model programs exist and, if they do, are they being adapted to meet local cybersecurity needs?
- What partnerships should two-year and four-year colleges and universities forge with business and industry to build appropriate programs? In your opinion, is there sufficient collaboration with industry at the administration (advisory committees), faculty (return-to-industry) and student (internship) levels to accommodate rapid changes in these professional and technical areas?
- What can the federal government do to improve cybersecurity education and build the Nation's technical workforce?

Questions for Mr. Baker

- What are the various levels of cybersecurity education and training, e.g., systems administration, systems engineering, and systems architecture? What role does your university play in this education and training continuum? How do two- and four-year colleges and institutions collaborate—if at all—to identify and fill cybersecurity educational needs?

[2] NSA competitively awards a small amount of funding (a few million dollars) for capacity building—curriculum development, purchase of infrastructure for courses—at CAE/IAE schools.

- What are the current strengths and weaknesses of cybersecurity education and training programs? What courses and programs currently exist? And what programs need to be developed and more broadly implemented?
- What are the challenges to faculty preparation, recruitment and retention in cybersecurity? How has your university attempted to address these challenges?
- What can the federal government do to improve cybersecurity education and build the Nation's technical workforce?

Questions for Mr. Spengler

- What role do community colleges play in the training of new workers and the retraining of current workers? What employment opportunities in cybersecurity are available for individuals with a certificate or a two-year degree?
- What are the current strengths and weaknesses of cybersecurity education and training programs? What "model" courses and programs currently exist? And what types of courses or programs need to be developed or more broadly implemented?
- What are the challenges do you face in recruiting and training cybersecurity faculty? What type of programs or opportunities do you provide to help keep faculty current?
- What can the federal government do to improve cybersecurity education and build the Nation's technical workforce?

Questions for Lt. Aparicio

- How did your experience at the ACE change your view of cybersecurity issues? Is this a good way to recruit engineering and other science and technology students into the field? How did your experience in the course influence your career plans?
- Do you think that the combination of education, problem solving and immersion is an effective model for other education and training programs? Why or why not?
- In your opinion, what can the federal government do to improve cybersecurity education and build the Nation's technical workforce?

Questions for Ms. Rogers

- What role do community colleges play in the training of new workers and the retraining of current workers? What employment opportunities in cybersecurity are available for individuals with a certificate or a two-year degree?
- What are the current strengths and weaknesses of cybersecurity education and training programs? What "model" courses and programs currently exist? And what types of courses or programs need to be developed or more broadly implemented?
- What are the challenges do you face in recruiting and training cybersecurity faculty? What type of programs or opportunities do you provide to help keep faculty current?
- What can the federal government do to improve cybersecurity education and build the Nation's technical workforce?

Appendix I: NSF ATE Award Abstracts

Tennessee Information Technology (TN IT) Exchange Center

Start Date September 15, 2002
Expires August 31, 2005 (Estimated)
Expected Total Amount $1798803 (Estimated)
Investigator Sydney U. Rogers sydney.rogers@nscc.edu (Principal Investigator current))
Sponsor Nashville St Tech Community College
120 White Bridge Rd
Nashville, TN 372094515 615/353-3236

The Tennessee Information Technology (IT) Exchange Center provides an effective workforce capacity building system by increasing the IT educational strength in a consortium of two year colleges, four year colleges, secondary schools and industries in North Central Tennessee. The goal is to develop a sustainable Center to meet the needs of industry for a qualified IT workforce by creating real world scenarios based on industrial needs and using them as the basis for instruction in IT courses. The learning strategies are developed in workshops at the Center for Learning and Teaching at Vanderbilt University. The cases are used in high school academies to interest high school students in IT careers. A web site provides information about the availability and content of education and training programs in the region, a clearinghouse of job opportunities and regular communications among partners. Regional stakeholder forums bring industry and educators together to develop a shared vision based upon research for effective delivery of instruction. The audience includes both students in educational institutions and re-careering workers.

Center for the Advancement of Systems Security and Information Assurance (CASSIA)

Start Date September 1, 2003
Expires August 31, 2007 (Estimated)
Expected Total Amount $2997615 (Estimated)
Investigator Erich Spengler spengler@morainevalley.edu (Principal Investigator current)

Sponsor Moraine Valley Community College
10900 South 88th Avenue
Palos Hills, IL 604652175 708/974-4300

This regional center for information technology (IT) security and data assurance serves a five-state area of the Midwest and focuses on a field which is critical to homeland security and which has a large demand for qualified workers. The center builds on a

previous Advanced Technological Education project at Moraine Valley Community College, "Applied Internet Technology: Curriculum and Careers" (NSF Award No. 9950037; see http://www.fastlane.nsf.gov/servlet/showaward?award=9950037 and http://www.morainevalley.edu/nsf/), which concluded in 2002. The following educational institutions are collaborating in the operation of the center: Moraine Valley Community College, Rock Valley College, University of Illinois at Springfield, Lakeland Community College, Washtenaw Community College, Inver Hills Community College, and Madison Area Technical College. Other organizations from business, industry, and government are also advising the center and participating in its activities.

The center is collecting, adapting, and enhancing curricula in cybersecurity, offering certificate and degree programs, and providing professional development for college faculty in the region. In particular, the center is establishing an A.A.S. degree and a certificate in IT security and data assurance; a concentration in IT security and data assurance within a B.S. degree program in computer science; an Internet-accessible laboratory environment that demonstrates and simulates security technologies; "train the trainer" summer workshops and externship opportunities for faculty from regional community colleges and four-year institutions; an internship program for students in the A.A.S. and B.S. degree programs; and a comprehensive outreach and support program to increase the number of students from underrepresented groups who pursue IT careers.

Appendix II. Institutions Involved in NSF's Cybersecurity Scholarships for Service Program

Institutions with Students in NSF's Cybersecurity Scholarships for Service Program[3]

Carnegie Mellon University
Clark Atlanta University
Florida State University
George Washington University
Georgia Institute of Technology
Idaho State University
Iowa State University
Jackson State University
Johns Hopkins University
Morehouse College
Mississippi State University
Naval Postgraduate School
New Mexico Institute of Mining & Technology
Norwich University
Polytechnic University
Purdue University
Spelman College
SUNY at Stony Brook

[3] NSF does not directly fund students in the Scholarships for Service program. Instead, funding is provided to institutions who select the scholarship recipients.

Syracuse University
University of Idaho
University of Nebraska at Omaha
University of North Carolina at Charlotte
North Carolina A&T University
University of Tulsa

Institutions Receiving Capacity Building Grants via NSF's Cybersecurity Scholarships for Service Program

Adelphi University
Amherst College
California State at Long Beach
Carnegie Mellon University
Clark Atlanta University
CUNY Brooklyn
CUNY Borough of Manhattan Community College
CUNY NYC College of Technology
Embry Riddle Aeronautical University
Florida Agricultural and Mechanical University
Florida State University
George Washington University
Georgia Institute of Technology
Hampshire College
Indiana University of Pennsylvania
Illinois Institute of Technology
Indiana University
Iowa State University
Jackson State University
John Jay College of Criminal Justice
Kentucky State University
Mississippi State University
Mount Holyoke College
Murray State University
Naval Postgraduate School
New Mexico Institute of Mining and Technology
North Carolina Agricultural and Technical State University
North Dakota State University at Fargo
Pennsylvania State University
Polytechnic University
Purdue University
Smith College
Stevens Institute of Technology
SUNY Albany
SUNY at Stony Brook
Texas A&M

University of Alaska-Fairbanks
University of Denver
University of Houston
University of Idaho
University of Kansas
University of Louisville Research Foundation
University of Massachusetts at Amherst
University of Missouri
University of North Carolina at Charlotte
University of Pittsburgh
University of Rhode Island
University of Southern California
University of South Carolina at Columbia
University of Washington
University of Wisconsin-Stevens Point
University of Wisconsin-Parkside
University of Wisconsin-Milwaukee
Towson University
Utica College
Wichita State University

Appendix III: NSA Centers of Academic Excellence in Information Assurance Education

Alabama
Auburn University

California
Naval Postgraduate School
Stanford University
University of California at Davis

Florida
Florida State University

Georgia
Georgia Institute of Technology
Kennesaw State University

Idaho
Idaho State University
University of Idaho

Illinois
University of Illinois at Urbana-Champaign

Indiana
Purdue University

Iowa
Iowa State University

Maryland
Capitol College
Johns Hopkins University
Towson University
University of Maryland, Baltimore County
University of Maryland University College

Massachusetts
Boston University
Northeastern University
University of Massachusetts, Amherst

Michigan
University of Detroit, Mercy
Walsh College

Mississippi
Mississippi State University

Nebraska
University of Nebraska at Omaha

New Jersey
New Jersey Institute of Technology
Stevens Institute of Technology

New Mexico
New Mexico Tech

New York
Pace University
Polytechnic
State University of New York, Buffalo
State University of New York, Stony Brook
Syracuse University
U.S. Military Academy, West Point

North Carolina
North Carolina State University
University of North Carolina, Charlotte

Ohio
Air Force Institute of Technology

Oklahoma
University of Tulsa

Oregon
Portland State University

Pennsylvania
Carnegie Mellon University
Drexel University
East Stroudsburg University
Indiana University of Pennsylvania
Pennsylvania State University
University of Pennsylvania
University of Pittsburgh
West Chester University of Pennsylvania

South Dakota
Dakota State University

Texas
Texas A&M University
University of Dallas
University of North Texas
University of Texas, Dallas
University of Texas, San Antonio

Vermont
Norwich University

Virginia
George Mason University
James Madison University
University of Virginia

Washington
University of Washington

Washington, D.C.
George Washington University
Information Resources Management College